

セキュリティ管理システムおよび方法

BACKGROUND OF THE INVENTION

本発明は、ネットワークに接続した各種処理装置からなる情報処理システムのセキュリティ状態の制御および管理を支援する技術に関する。

近年、インターネット技術等を用いた情報システムが企業活動のインフラとして広く活用されるようになったことに伴い、情報システムに対する不正アクセスやウィルスによる情報資産への脅威を回避するためのセキュリティシステムの重要性が一段と高まっている。

このようなセキュリティシステムを管理するための従来の技術としては、ファイアウォールやウィルス対策プログラムなどの、情報システム上の個々のセキュリティシステムの設定や変更を行うTivoli社の製品Tivoli Security Managementなどが知られている。

SUMMARY OF THE INVENTION

さて、情報システムのセキュリティ対策は、情報システム全体の脅威分析に基づく対策方針である情報セキュリティポリシーの作成、情報セキュリティポリシーに従ったセキュリティシステムの情報システムへの導入および運用管理といった一連の手順を経て実施することが望まれている。このような手順に沿った情報システムのセキュリティ対策を推奨するものとしては、1999年6月にISO15408として国際標準化されたセキュリティ評価基準CC(Common Criteria)がある。

しかしながら、上記技術によれば、情報セキュリティポリシーに従ったセキュリティ対策を実現するために導入したセキュリティシステムが何であるのかや、各情報セキュリティポリシーに対してセキュリティシステムをどのように運用管理しているのかなどを管理するための仕組みがない。

このため、情報セキュリティポリシーに従った情報システムのセキュリティの状態の制御や管理は、情報セキュリティポリシーならびにセキュリティシステムに関する高度な専門知識を有する管理者でなければ、行うことが困難であった。また、情報セキュリティポリシーに従った情報システムのセキュリティ状態の制御や管理に要する時間やコストなどの負担が大きかった。

上記事情に鑑みてなされたものであり、本発明は、情報セキュリティポリシーに従った、情報システムのセキュリティの状態の制御や管理を簡単にする技術（システム、ソフトウェア等を含む）を提供する。

また、本発明は、情報セキュリティポリシーならびにセキュリティシステムに関する高度な専門知識がなくても、情報セキュリティポリシーの作成、情報セキュリティポリシーに従ったセキュリティシステムの情報システムへの導入および運用管理といった一連の手順を実施できるように支援にする技術（システム、ソフトウェア等を含む）を提供する。

また、本発明は、これらの技術を用いて、セキュリティシステムの構築サービスを提供する。

本発明の第1の態様は、少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキュリティ状態を、当該対応する情報セキュリティポリシーに整合するように制御する、複数

の管理部を用意する。そして、ユーザより受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応する管理部を抽出して、当該管理部に、当該管理部に対応する被管理対象システムのセキュリティ状態を、当該管理部に対応する情報セキュリティポリシーに整合するように変更させる。

あるいは、少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティの状態を監査する、複数の監査部を用意する。そして、ユーザより受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応する監査部を抽出して、当該監査部に、当該監査部に対応する被管理対象システムの当該監査部に対応する情報セキュリティポリシーに関わるセキュリティ状態を監査させる。

また、本発明の第2の態様では、まず、セキュリティ施策のポリシーを表す情報セキュリティポリシーと、少なくとも1つの被管理対象システムとの対応が記述されたデータベースを用意する。そして、ユーザが構築したあるいは構築しようとしている情報システムを構成する各被管理対象システムの指定を受け付け、これらに対応付けられて登録されている情報セキュリティポリシーを前記データベースから抽出して、例えば当該情報システムを構成する被管理対象システムと情報セキュリティポリシーとの対応の一覧が記述された、当該情報システムに適用すべきセキュリティ仕様を策定する。

次に、策定したセキュリティ仕様により特定される情報セキュリティポリシーおよび管理対象システムの組に各々対応付けられた、当該被管理対象システムの型式やソフトウェアバージョンといった諸情報、および、当該被管理対象システムの当該情報セキュリティポリシーに関わるセキュリティ状態を監査するための処理が記述された複数の監査プログラムを、ユーザが構築した情報システムに導入したセキュリティ管理システムに実行させる。そして、ユーザが構築した情報システムを構成する各被管理対象システムの型式やソフトウェアバージョンといった諸情報およびセキュリティ状態を監査して、当該情報システムのセキュリティを診断する。

それから、策定したセキュリティ仕様により特定される情報セキュリティポリ

シーおよび管理対象システムの組に各々対応付けられた、当該被管理対象システムの対応する情報セキュリティポリシーに関わるセキュリティ状態を制御する処理が記述された複数の管理プログラムのうち、例えば、ユーザがセキュリティの診断結果からセキュリティ状態を変更する必要があると判断した情報セキュリティポリシーおよび管理対象システムの組に対応付けられている管理プログラムを、当該ユーザが構築した情報システムに導入したセキュリティ管理システムに実行させ、当該管理プログラムに対応する被管理対象システムのセキュリティ状態を、当該管理プログラムに対応する情報セキュリティポリシーに整合するように変更させる。

BRIEF DESCRIPTION OF THE DRAWINGS

図 1 は、本発明の第 1 実施形態が適用された情報システムの概略構成図である。

図 2 は、図 1 に示す情報セキュリティポリシー管理・監査支援装置 31 の概略構成図である。

図 3 は、図 1 に示す管理・監査対象計算機 32 の概略構成図である。

図 4 は、図 2 に示すシステム構成機器情報データベース 131 の内容を説明するための図である。

図 5 は、図 2 に示す情報セキュリティポリシーデータベース 132 の内容を説明するための図である。

図 6 は、図 2 に示すセキュリティ管理・監査プログラムデータベース 133 の内容を説明するための図である。

図 7 は、図 1 に示す情報セキュリティポリシー管理・監査支援装置 31 の動作手順を示すフロー図である。

図 8 は、図 7 のステップ S701 で表示される、情報セキュリティポリシー管理・監査対象領域選択画面を示す図である。

図 9 は、図 7 のステップ S703 で表示される、情報セキュリティポリシー選択画面を示す図である。

図 10 は、図 7 のステップ S705 における処理手順を示すフロー図である。

図 11 は、図 7 のステップ S706 で表示される、情報セキュリティポリシーの実施状況/セキュリティ施策の変更画面を示す図である。

図 12 は、管理プログラムが起動された場合の表示画面例を示す図である。

図 13 は、監査プログラムの起動された場合の処理手順例を示すフロー図である。

図 14 は、情報セキュリティポリシーの監査結果表示画面を示す図である。

図 15 は、情報セキュリティポリシーの監査結果表示画面を示す図である。

図 16 は、情報セキュリティポリシーの監査結果表示画面を示す図である。

図 17 は、情報セキュリティポリシーの監査結果表示画面を示す図である。

図 18 は、本発明の第 2 実施形態で用いる情報セキュリティポリシー管理・監査支援装置 31' の概略構成図である。

図19は、図18に示す管理・監査対象システムの構成機器情報/セキュリティ状態データベース135の内容を説明するための図である。

図20は、図18に示すセキュリティポリシー管理・監査支援装置31'を用いることで実現可能な、情報システムのセキュリティ管理の支援手順を、概念的に表した図である。

図21は、図20に示す設計フェーズでのセキュリティポリシー管理・監査装置31'の動作手順を示すフロー図である。

図22は、セキュリティ仕様書の一例を示す図である。

図23は、図20に示す導入フェーズでのセキュリティポリシー管理・監査装置31'の動作手順を示すフロー図である。

図24は、監査結果報告書の一例を示す図である。

図25は、不正アクセスの履歴が監査結果2403として表示される場合の監査結果報告書の一例を示す図である。

図26は、図20に示す運用フェーズでのセキュリティポリシー管理・監査装置31'の動作手順を示すフロー図である。

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

以下、本発明の実施の形態について説明する。

まず、本発明の第1実施形態について説明する。

図1は、本発明の第1実施形態が適用された情報システムの構成図である。

図示するように、本実施形態の情報システムは、情報セキュリティポリシー管理・監査支援装置31と、サーバやルータやファイアウォールなどの管理・監査対象計算機32とが、ネットワーク33を介して接続された構成を有している。

図2に、情報セキュリティポリシー管理・監査支援装置31の構成を示す。

図示するように、情報セキュリティポリシー管理・監査支援装置31のハードウェア構成は、たとえば、CPU11と、メモリ12と、ハードディスク装置などの外部記憶装置13と、ネットワーク33に接続された通信装置14と、キーボードやマウスなどの入力装置15と、ディスプレイなどの表示装置16と、FDやCD-ROMなどの可搬性を有する記憶媒体からデータを読み取る読取り装置17と、上述した各構成要素間のデータ送受信を司るインタフェース18とを備えた、一般的な電子計算機上に構築することができる。

ここで、外部記憶装置13上には、情報セキュリティポリシー管理・監査支援装置31の各機能を電子計算機上に構築するための支援プログラム134が格納されている。CPU11は、このプログラム134をメモリ12上にロードし実行することにより、管理・監査対象領域制御部111、情報セキュリティポリシー選択制御部112、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113、および、入出力制御部114を、電子計算機上に実現する。また、外部記憶装置13上に、システム構成機器情報データベース131、情報セキュリティデータベース132、および、セキュリティ管理・監査プログラムデータベース133を形成する。また、図示は省略したが、電子計算機上には、ネットワーク33を介して他装置と相互に通信するための通信制御部なども構築される。

図3に、管理・監査対象計算機32の構成を示す。

ここで、図2に示す情報セキュリティポリシー管理・監査支援装置31と同じ機能を有するものには同じ符号を付している。

図示するように、管理・監査対象計算機32の外部記憶装置13には、管理・監査

対象計算機32上で稼動するOSプログラム150と、アプリケーションプログラム137と、アプリケーションプログラム137のセキュリティ管理・監査を行うセキュリティ管理・監査プログラム群136が格納されている。

CPU11は、メモリ12上にロードされたOSプログラム150を実行することにより、OS151を電子計算機上に実現する。また、メモリ12上にロードされたアプリケーションプログラム137を実行することにより、サーバやルータやファイアウォールなどが有する個々のサービスを提供するアプリケーション部138を電子計算機上に実現する。また、メモリ12上にロードされたセキュリティ管理・監査プログラム群136に含まれる管理プログラムを実行することにより、OS151やアプリケーション部138のセキュリティ施策の状態を設定変更するセキュリティ管理部139を電子計算機上に実現し、セキュリティ管理・管理プログラム群136に含まれる監査プログラムを実行することにより、OS151やアプリケーション部138のセキュリティ施策の状態を確認するセキュリティ監査部140を電子計算機上に実現する。また、図示は省略したが、電子計算機上には、ネットワーク33を介して他装置と相互に通信するための通信制御部なども構築される。

次に、情報セキュリティポリシー管理・監査支援装置31の各データベースについて説明する。

図4に、システムの構成機器情報データベース131の内容を示す。

図中、各行において、列41には、情報セキュリティポリシー管理・監査の対象となるシステムを一意に識別する識別子(SYSID)が記述される。列44には、列41のSYSIDで示されるシステムを構築するソフトウェアプログラム名(OSプログラム150やアプリケーションプログラム137の名称)が記述される。列42には、列41のSYSIDで示されるシステムが稼動する装置の種別(例えば、ルータ、サーバ、クライアント、ファイアウォールなど)が記述される。そして、列45には、列41のSYSIDで示されるシステムの操作者による選択結果が格納される。

図5に、情報セキュリティポリシーデータベース132の内容を示す。

図中、各行において、列51には、情報セキュリティポリシーを一意に識別する識別子(POLICYID)が記述される。列52には、列51のPOLICYIDの欄に記述された情報セキュリティポリシーの施策種別(例えば、識別と認証、アクセス制御機能な

ど)が記述される。列53には、列51のPOLICYIDの欄に記述された情報セキュリティポリシーの内容を表すセキュリティ施策(例えば、ネットワークにアクセス可能な端末の限定、識別・認証情報用の良いパスワード設定の実施など)が記述される。そして、列54には、列51のPOLICYIDで示される情報セキュリティポリシーの操作者による選択結果が格納される。

図6に、セキュリティ管理・監査プログラムデータベース133の内容を示す。

図中、各行において、列61には、情報セキュリティポリシーを一意に識別する識別子(POLICYID)が記述される。列62の管理プログラムの欄には、列61のPOLICYIDの欄に記述された情報セキュリティポリシーのセキュリティ施策の管理を行う管理プログラムの名称621と、名称621の管理プログラムが管理を行うシステムのSYSID622と、名称621の管理プログラムの実行要否を表す対応付け623が記述される。そして、列63の監査プログラムの欄には、列61のPOLICYIDの欄に記述された情報セキュリティポリシーのセキュリティ施策の監査を行う監査プログラムの名称631と、名称631の監査プログラムが監査を行うシステムのSYSID632と、名称631の監査プログラムの実行要否を表す対応付け633が記述される。

以下、このような情報システムにおける、セキュリティポリシー管理・監査の動作について説明する。

図7に、セキュリティポリシー管理・監査装置31の動作手順を示す。

まず、管理・監査対象領域制御部111は、入出力制御部114を用いて、表示装置16に、図8に示すような、外部記憶装置13上に形成されているシステム構成機器情報データベース131に登録されている内容を表した情報セキュリティポリシー管理・監査対象領域選択画面を表示する(ステップS701)。

図8において、「装置種別」91、「ソフトウェア種別」92および「プログラム名」93の各項目は、システム構成機器情報データベース131の列42、43、44に、それぞれ対応している。この画面上で、操作者は、任意の項目91～93で情報セキュリティポリシー管理・監査対象領域を指定し、これを項目「使用可否」94のボタンで選択できる。この選択結果は、管理・監査対象領域制御部111によって、システム構成機器情報データベース131の列45に反映される。すなわち、ある装置種別が選択された場合にはその装置種別が記述された全ての行の列45に、また、

あるソフトウェア種別が選択された場合にはそのソフトウェア種別が記述された全ての行の列45に、さらに、あるプログラム名が選択された場合にはそのプログラム名が記述された行の列45に、選択可否として「YES」を登録する。

次に、操作者によって情報セキュリティポリシー管理・監査対象領域が選択されると、(ステップS702)、情報セキュリティポリシー選択制御部112は、入出力制御部114を用いて、表示装置16に、図9に示すような、情報セキュリティポリシーデータベース132に登録されている内容を表した情報セキュリティポリシー選択画面を表示する(ステップS703)。

図9において、「施策種別」1001および「セキュリティ施策」1002の各項目は、情報セキュリティポリシーデータベース132の列52、53に、それぞれ対応している。この画面上で、操作者は、任意の項目1001、1002で情報セキュリティポリシーを指定し、これを項目「使用可否」1003のボタンで選択できる。この選択結果は、情報セキュリティポリシー選択制御部112によって、情報セキュリティポリシーデータベース132の列54に反映される。すなわち、ある施策種別が選択された場合にはその施策種別が記述された全ての行の列54に、また、あるセキュリティ施策が選択された場合にはそのセキュリティ施策が記述された行の列54に、選択可否として「YES」を登録する。

次に、操作者によって情報セキュリティポリシーが選択されると(ステップS704)、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、ステップS701～S704により選択された結果に基づき、選択された情報セキュリティポリシーとシステムに対応する管理・監査プログラムを、セキュリティ管理・監査プログラムデータベース133から抽出する。そして、抽出した管理・監査プログラムの対応付けの列623、633に「要」を登録する(ステップS705)。

この抽出は、図10に示す手順によって行う。

すなわち、セキュリティ管理・監査プログラムデータベース133において、まず、情報セキュリティポリシーの検索を、列61を対象にして、ステップS704で選択された(情報セキュリティポリシーデータベース132において列54に「YES」が登録されている)識別子(POLICYID)の有無を用いて行う(ステップS801)。次に、

管理プログラムの抽出を、検索した識別子(POLICYID)と同じ行にある列622を対象にして、ステップS702で選択されたシステム(システム構成機器情報データベース131において列54に「YES」が登録されている)の識別子(SYSID)の有無を用いて行う(ステップS802、S803)。それから、監査プログラムの抽出を、検索された識別子(POLICYID)と同じ行にある列632を対象にして、ステップS702で選択されたシステム(システム構成機器情報データベース131において列「54」にYESが登録されている)の識別子(SYSID)の有無を用いて行う(ステップS804、S805)。

さて、図7に戻り、管理・監査プログラムの抽出が終わると、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、入出力制御部114を用いて、表示装置16に、図11に示すような、情報セキュリティポリシーの実施状況ならびにセキュリティ施策の変更を指定するための画面を表示する(ステップS706)。

図11において、「施策種別」1001および「セキュリティ施策」1002の各項目は、情報セキュリティポリシーデータベース132の列52、53に、それぞれ対応しており、ステップS704で選択された(YESが列54に設定された)もののみが表示される。操作者は、「施策種別」1001および「セキュリティ施策」1002の各項目において、管理や監査の対象となる情報セキュリティポリシーを1あるいは複数選択することができる。また、項目「管理」1101は、情報セキュリティポリシーの選択後、管理プログラムを用いて、選択した情報セキュリティポリシーに関わるセキュリティ施策の変更を行うためのボタンであり、項目「監査」1102は、情報セキュリティポリシーの選択後、監査プログラムを用いて、選択した情報セキュリティポリシーに関わる情報セキュリティポリシーの実施状況を確認するためのボタンである。操作者は、「管理」1101および「監査」1102のいずれかのボタンを選択できる。

さて、操作者により、情報セキュリティポリシーが選択され、そして、「管理」1101および「監査」1102のいずれかのボタンが選択されると(ステップS707)、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、ステップS705において、選択された情報セキュリティポリシーに対して抽出された(セキュリティ管理・監査プログラムデータベース133の対応付けの

列623、633に「要」がマークされた）、セキュリティ管理プログラムあるいは監査プログラムを、ネットワーク33を介して起動する。

選択されたボタンが「管理」1101である場合、管理・監査対象計算機32上の管理・監査プログラム群136のうち、上記のようにして抽出された管理プログラムが起動され、実行される。管理プログラムの実行により具現化するセキュリティ管理部139は、管理・監査対象計算機32の表示装置16上に、たとえば図12に示すような、セキュリティシステムの設定変更などの管理画面を表示する（ステップS708）。そして、セキュリティシステムの設定変更を受付て設定し、その内容をネットワーク33を介して情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113に応答する。応答を受けた情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、その内容を情報セキュリティポリシー管理・監査支援装置31の表示装置16上に表示する。

なお、図12は、図5に示す情報セキュリティポリシーデータベース132において、施策種別52「識別と認証機能」、セキュリティ施策53「識別・認証情報用の良いパスワード設定の実施」に対応する情報セキュリティポリシー「AUTH-01」を管理する管理プログラムである、パスワード管理プログラム（図6の管理プログラム名621「ADM_USR_#2」）が起動された場合の例を示している。図12の画面は、パスワードの設定変更を受け付ける画面である。

一方、ステップS707において、選択されたボタンが「監査」1102である場合、管理・監査対象計算機32上の管理・監査プログラム群136のうち、上記のようにして抽出された監査プログラムが起動され、たとえば、図13に示すような動作手順によって、その監査プログラムが監査を行うシステムのセキュリティ監査を行う（ステップS709）。そして、その結果を、ネットワーク33を介して、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113に応答する。応答を受けた情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、その内容を情報セキュリティポリシー管理・監査支援装置31の表示装置16に表示する。

なお、図13は、図5に示す情報セキュリティポリシーデータベース132において、施策種別52「アクセス監視」、セキュリティ施策53「データ・プログラム

の改ざん検出の実施」に対応する情報セキュリティポリシー「ACCADM-01」を管理する監査プログラムである、データ改ざん監査プログラム（図6の管理プログラム名621「AUDIT_LOG_#1」）が起動された場合の例を示している。この例では、監査プログラムは、改竄検出プログラム自体が管理・監査対象計算機32上にインストールされ稼動されているか否かを確認し（ステップS1701）、次に、その稼動動作ログが保存されているかを確認する（ステップS1702）。それから、稼動動作ログの更新日を確認することで改ざん検出プログラムの継続稼動を確認する（ステップS1703）。そして、全ての確認項目に対して確認できたならば、監査結果は良好であるので、監査結果として「実施済」を情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113に応答する（ステップS1705）。一方、そうでないならば、監査結果は不良となるので、監査結果として「実施未」を情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113に応答する（ステップS1704）。

さて、図7に戻り、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、監査結果の応答を受けとると、それを表示装置16に表示する（ステップS710）。

以上、本発明の第1実施形態について説明した。

ところで、本実施形態では、図4のプログラム名44に記述されるプログラムを単位として、管理・監査プログラムを設けた場合について説明した。しかしながら本発明はこれに限定されない。たとえば、図4に示すシステムの構成機器情報データベース131において、装置種別42に記述される装置やソフトウェア種別43に記述されるソフトウェアを単位として、この単位毎に管理・監査プログラムを設け、選択された装置種別やソフトウェア種別とセキュリティ施策に応じて、管理・監査プログラムを実行するようにしてもよい。

なお、装置種別を単位として、管理・監査プログラムを設ける場合、監査結果の表示は、たとえば、次のように行うことができる。

図14は、監査結果を、図4に示すシステムの構成機器情報データベース131の装置種別42毎に、図5に示す情報セキュリティポリシーデータベースの施策種別52毎の、当該施策種別の全セキュリティ施策数53に対する実施済の割合を、い

わゆるレーダーチャートを用いて表示する例を示している。また、図15は、前記実施済の割合を表を用いて表示する例を示している。

図14あるいは図15において、操作者は、タグ1201を指定することで、装置種別42毎の監査結果を表示させることができる。また、操作者が、施策種別1202を指定し、ボタン「詳細」1203を選択したならば、図17に示すような、図5に示す情報セキュリティポリシーデータベースの施策種別52毎に、セキュリティ施策53毎の応答された監査結果を表示する。

図17において、操作者は、監査結果に基づき、設定変更などの管理を実施したい場合や、再度、監査を実施したい場合、列1402の選択欄をチェックし、管理プログラムを用いてセキュリティ施策の変更を行うためのボタン「管理」1402、あるいは、監査プログラムを用いて情報セキュリティポリシーの実施状況の確認を行うためのボタン「監査」1403を選択することができる。

図16は、監査結果を、図5に示す情報セキュリティポリシーデータベースの施策種別52毎に、図4に示すシステムの構成機器情報データベース131の装置種別42毎の、当該施策種別の全セキュリティ施策数53に対する実施済の割合を、いわゆるレーダーチャートを用いて表示する例を示している。

図16において、操作者は、タグ1501を指定することで、施策種別52毎の監査結果を表示させることができる。また、操作者が、装置種別1502を指定し、ボタン「詳細」1503を選択したならば、図17に示すような、図5に示す情報セキュリティポリシーデータベースの施策種別52毎に、セキュリティ施策53毎の応答された監査結果を表示する。

さて、本実施形態によれば、以下のような効果がある。

(1)操作者が管理・監査対象となるシステムを指定し、情報セキュリティポリシーを選択するだけで、その構成で必要となるセキュリティ管理・監査プログラムが選択される。このため、情報セキュリティポリシーに従ったセキュリティ対策を実現するために導入したセキュリティシステムとの対応付けが容易となる。

(2)操作者が入力した情報セキュリティポリシーの管理実施を指定するだけで、その対象システムの情報セキュリティポリシーの適用を行う管理プログラムを起動することができる。このため、情報セキュリティポリシーに従った情報シス

ムの運用管理を行うために、高度な専門知識を有しない管理者の場合にも、運用管理が容易となる。

(3) 操作者が入力した情報セキュリティポリシーの状態を監査実施を指定するだけで、その対象システムの情報セキュリティポリシーに基づくセキュリティ施策の状態を評価することができる。このため、情報セキュリティポリシーに従った情報システムの運用管理状態を把握するために、高度な専門知識を有しない管理者の場合にも実施が容易となる。

次に、本発明の第2実施形態について説明する。

本実施形態では、上記の第1実施形態で説明したセキュリティポリシー管理・監査支援装置31に若干の修正を加え、この修正された装置31'を用いて、管理者が、ユーザの情報システムに適用すべき情報セキュリティポリシーの作成、当該情報セキュリティポリシーに従ったセキュリティシステムの前記情報システムへの導入および運用管理といった一連の手順を実施できるように支援する場合について説明する。

図18に、セキュリティポリシー管理・監査支援装置31'の構成を示す。

図示するように、本実施形態で用いるセキュリティポリシー管理・監査支援装置31'の構成は、図2に示す第1実施形態のものと基本的に同様である。ただし、CPU11が、外部記憶装置13上に格納されている支援プログラム134をメモリ12上にロードし実行することにより、外部記憶装置13上に、システム構成機器情報データベース131、情報セキュリティデータベース132およびセキュリティ管理・監査プログラムデータベース133に加えて、管理・監査対象システムの構成機器情報/セキュリティ状態データベース135が形成される。このデータベース135には、図6に示したセキュリティ管理・監査プログラムデータベース133において対応付けがされている監査プログラムの実行により当該プログラムの監査対象システムから入手した、当該システムに対するセキュリティ施策の状態と、当該システムを構築するソフトウェアプログラムのバージョン情報や当該システムが稼動する装置の型式といった諸情報が格納される。

図19に、管理・監査対象システムの構成機器情報/セキュリティ状態データベース135の内容を示す。

図中、各行において、列71には、監査プログラムの名称(AUDITID)が記述される。列72には、列71の対応する欄に記述されたAUDITIDにより特定される監査プログラムが対応するシステムのSYSID721（セキュリティ管理・監査プログラムデータベース133より特定できる）と、当該監査プログラムの実行によりSYSID721で示されるシステムから入手した、当該システムを構築するソフトウェアプログラムのソフトウェア種別722、プログラム名称723およびバージョンやパッチといった更新情報724と、当該システムが稼動する装置の種別725および型式情報726とを含む、当該監査プログラムが監査対象とするシステムの最新の諸情報が記述される。また、列73には、列71の対応する欄に記述されたAUDITIDにより特定される監査プログラムの実行により入手した、図6に示したセキュリティ管理・監査プログラムデータベース133において当該監査プログラムに対応付けられているPOLCYID61により特定される情報セキュリティポリシーが示すセキュリティ施策（情報セキュリティポリシーデータベース132より特定できる）の実施の有無731と、当該システムの当該セキュリティ施策に関するセキュリティ状態732とを含む、当該監査プログラムが監査対象とするシステムに対するセキュリティ情報が記述される。ここで、セキュリティ状態732としては、例えば、セキュリティ施策が「外部ネットワークにアクセス可能な端末の限定」であり、監査対象とするシステムが「ルータ」の場合、当該ルータの外部ネットワークへの接続に関する設定情報が該当する。セキュリティ状態732として、どのような情報を入手するかは、監査プログラム毎に、当該監査プログラムが監査するシステムや情報セキュリティポリシー等によって定まる。

次に、このセキュリティポリシー管理・監査支援装置31'を用いることで実現できる情報システムのセキュリティ管理の支援について説明する。

図20は、セキュリティポリシー管理・監査支援装置31'を用いることで実現可能な情報システムのセキュリティ管理の支援手順を概念的に表した図である。

図示するように、本実施形態による情報システムのセキュリティ管理の支援手順は、以下の3つのフェーズに分かれる。

①設計フェーズ

セキュリティポリシー管理・監査支援装置31'を用いて、ユーザが構築したあ

るいは構築しようとしている情報システムの仕様を受け付け（2001）、当該情報システムに適用可能なセキュリティ仕様を策定する。そして、このセキュリティ仕様をユーザに提示して（2002）、当該情報システムに適用する情報セキュリティポリシーを決定し、この決定された情報セキュリティポリシーに従ったセキュリティ施策の監査・管理を行えるように情報セキュリティポリシー管理・監査支援装置31'を設定する（2003）。

②導入フェーズ

ユーザの情報システムにセキュリティポリシー管理・監査支援装置31'を接続する（2004）。そして、当該情報システムの、設計フェーズで決定された情報セキュリティポリシーに関するセキュリティ状態を診断し（2005、2006）、必要に応じて、当該システムのセキュリティ状態を変更する（2007、2008）。

③運用フェーズ

ユーザの情報システムの、設計フェーズで決定された情報セキュリティポリシーに関するセキュリティ状態を定期的に診断し（2009、2010）、導入フェーズ後に、ソフトウェアバージョン、型式といった諸情報あるいはセキュリティ状態に変更があった箇所を特定し（2011）、必要に応じて当該箇所のセキュリティ状態を変更する（2012）。また、セキュリティ状態の診断結果とCERT(Computer Emergency Response Team)等のセキュリティ情報機関が公表したセキュリティホール情報とを照合し（2013）、セキュリティ状態を変更する必要性が生じた箇所を特定して（2011）、そのセキュリティ状態を変更する（2012）。

なお、管理者は、ユーザの情報システムから入手したセキュリティ診断結果（2010）とセキュリティ情報機関が公表したセキュリティホール情報（2013）が、構成機器情報データベース131、情報セキュリティポリシーデータベース132、および、セキュリティ管理・監査プログラムデータベース133に反映されるように情報セキュリティポリシー管理・監査支援プログラム134を更新することにより、今後、新たにユーザの情報システムへ導入するセキュリティシステムにその内容が反映されるようにするとよい（2014）。

次に、図20に示した設計、導入および運用の各フェーズでのセキュリティポリシー管理・監査装置31'の動作について説明する。

まず、設計フェーズでの動作について説明する。

図 2 1 に、設計フェーズでのセキュリティポリシー管理・監査装置31'の動作手順を示す。この手順は、通常、セキュリティポリシー管理・監査装置31'がユーザの情報システムに接続されていない状態（この段階では、ユーザの情報システムが未だ構築されていない可能性がある）で行われる。

まず、管理・監査対象領域制御部111は、入出力制御部114を用いて、表示装置16に、図 8 に示したような、外部記憶装置13上に形成されているシステム構成機器情報データベース131に登録されている内容を表した情報セキュリティポリシー管理・監査対象領域選択画面を表示する（ステップS2101）。この画面上で、管理者は、ユーザより示された、当該ユーザが構築したあるいは構築しようとしている情報システムの構成機器を指定し選択することができる。この選択結果は、管理・監査対象領域制御部111によって、システム構成機器情報データベース131の列45に反映され、選択された構成機器（装置種別、ソフトウェア種別およびプログラム名の組み合わせで特定される）が記述された行の列45に、選択可否として「YES」が登録される。

次に、管理者によって、ユーザの情報システムの構成機器が選択されると、（ステップS2102）、情報セキュリティポリシー選択制御部112は、システム構成機器情報データベース131において列45に「Yes」が登録されているSYSIDに対応付けられているAUDITIDおよびPOLICYIDを、セキュリティ管理・監査プログラムデータベース133から検索する。

それから、情報セキュリティポリシー選択制御部112は、図 2 2 に示すような、システム構成機器情報データベース131において列45に「Yes」が登録されている行に記述された情報2201により特定される構成機器毎に、当該機器のSYSIDに対応付けられているPOLICYIDの施策種別およびセキュリティ施策（情報セキュリティポリシーデータベース132より特定できる）2202と、前記SYSIDおよび前記POLICYIDに対応付けられているAUDITIDの監査プログラムの監査（診断）項目（これは、監査プログラムに対応付けて外部記憶装置13等に予め格納しておくといよい）2203とを記述した、セキュリティ仕様書を作成する。そして、この作成したセキュリティ仕様書を、入出力制御部114を用いて表示装置16に表示したり、

あるいは、図示していない印刷装置から出力したりする（ステップS2103）。操作者は、このセキュリティ仕様書をユーザに提示することで、当該ユーザに、当該ユーザが構築したあるいは構築しようとしている情報システムに適用すべきセキュリティ施策を決定させることができる。

次に、情報セキュリティポリシー選択制御部112は、入出力制御部114を用いて、表示装置16に、図9に示したような、システム構成機器情報データベース131において列45に「Yes」が登録されている行の列41に記述されたSYSIDに対応付けられてセキュリティ管理・監査プログラムデータベース133に登録されているPOLICYIDの施策種別およびセキュリティ施策（情報セキュリティポリシーデータベース132より特定できる）を表した情報セキュリティポリシー選択画面を表示する（ステップS2104）。この画面上で、操作者は、ユーザより示された、当該ユーザが構築したあるいは構築しようとしている情報システムに適用すべき施策種別およびセキュリティ施策を指定し選択することができる。この選択結果は、情報セキュリティポリシーデータベース132の列54に反映され、選択された施策種別およびセキュリティ施策が記述された行の列54に、選択可否として「YES」が登録される。

次に、管理者によって、情報セキュリティポリシーが選択されると（ステップS2105）、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、ステップS2101～S2105により選択された結果に基づき、選択された情報セキュリティポリシーと構成機器とに対応する管理・監査プログラムを、セキュリティ管理・監査プログラムデータベース133から抽出する。そして、抽出した管理・監査プログラムの対応付けの列623、633に「要」を登録する（ステップS2106）。なお、この抽出手順は、先に図10で示した手順と同様である。

以上により、ユーザの情報システムに適用すべき情報セキュリティポリシー各々の実施状況を監査する監査プログラムとその状況を変更する管理プログラムが、セキュリティポリシー管理・監査装置31'に設定されたことになる。

次に、導入フェーズでの動作について説明する。

図23に、導入フェーズでのセキュリティポリシー管理・監査装置31'の動作手順を示す。この手順は、設計フェーズを経たセキュリティポリシー管理・監査

装置31'をユーザが構築した情報システムに接続したときに行われる。

まず、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、管理・監査対象計算機32上の管理・監査プログラム群136のうち、セキュリティ管理・監査プログラムデータベース133の対応付けの列633に「要」がマークされた監査プログラムを、ネットワーク33を介して起動し、管理・監査対象計算機32上にセキュリティ監査部140を構築する(ステップS2301)。

セキュリティ監査部140は、監査対象システムの構成機器の諸情報(監査対象システムを構築するソフトウェアプログラムのバージョン情報や監査対象システムが稼動する装置の型式といった情報を含む)とセキュリティ状態(監査プログラムに対応する情報セキュリティポリシーが示すセキュリティ施策の実施の有無と、当該セキュリティ施策に関連する監査対象システムのセキュリティ状況)とを監査する。そして、その監査結果をネットワーク33を介して情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113に応答する。情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、応答された監査結果に従い、管理・監査対象システムの構成機器情報/セキュリティ状態データベース135の内容を更新する(ステップS2302)。

次に、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、入出力制御部114を介して、管理者より監査結果報告指示を受け付けると(ステップS2303)、管理・監査対象システムの構成機器情報/セキュリティ状態データベース135の内容を、入出力制御部114を用いて、最新の監査結果報告書として、表示装置16に表示したり、あるいは、図示していない印刷装置から出力する(ステップS2304)。

図24に、監査結果報告書の一例を示す。図示するように、管理・監査対象システムの構成機器情報/セキュリティ状態データベース135の列72に記述されたシステム最新諸情報により特定される構成機器2401毎に、当該機器のSYSIDに対応付けられているPOLICYIDの情報セキュリティポリシーが示す施策種別およびセキュリティ施策(情報セキュリティポリシーデータベース132より特定できる)2402と、当該機器のSYSIDに対応付けられて列71に記述されているAUDITIDの監査プログラムの監査項目に対する監査(診断)結果2403とが記述される。なお、監

査結果2403は、管理・監査対象システムの構成機器情報/セキュリティ状態データベース135の列73に記述されたセキュリティ情報に基づいて作成される。上述したように、セキュリティ情報は、監査プログラムが監査するシステムや情報セキュリティポリシー等によって定まる。例えば、監査プログラムに対応付けられたSYSIDにより特定されるシステムがルータであり、監査プログラムに対応付けられたPOLICYIDの情報セキュリティポリシーが示す施策種別、セキュリティ施策がアクセス監視、不正アクセスの検知である場合、同じSYSIDおよびPOLICYIDに対応付けられた管理プログラムの起動により管理・監査対象計算機32上に構築されたセキュリティ管理部139が検知した不正アクセスの履歴がセキュリティ情報となる。この場合、図25に示すように、不正アクセスの履歴が監査結果2403として表示される。

さて、管理者は、この監査結果報告書から、設計フェーズにて、ユーザの情報システムに適用すべき旨決定した情報セキュリティポリシー各々が示すセキュリティ施策の実施状況を確認することができ、セキュリティ状態の変更が必要なシステム構成機器を特定することができる。

次に、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、入出力制御部114を介して、管理者よりセキュリティ状態の変更指示を受け付けると（ステップS2305）、入出力制御部114を用いて、表示装置16に、管理者が、セキュリティ管理・監査プログラムデータベース133の対応付けの列633に「要」がマークされた管理プログラムの中から所望の管理プログラムを選択して、セキュリティ施策の変更を指定するための画面を表示する（ステップS2306）。この画面では、セキュリティ管理・監査プログラムデータベース133の対応付けの列633に「要」がマークされた各管理プログラムに対応するPOLICYID61の情報セキュリティポリシーが示す施策種別およびセキュリティ施策（情報セキュリティポリシーデータベース132より特定できる）を一覧表示するとよい。このようにすれば、管理者は、変更したい施策種別およびセキュリティ施策を選択することで、管理プログラムに対する知識がなくても、当該セキュリティ施策を変更するための管理プログラムを選択することが可能となる。

さて、管理者により、管理プログラムが選択されると（ステップS2307）、情報

セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、管理・監査対象計算機32上の管理・監査プログラム群136のうち、選択された管理プログラムをネットワーク33を介して起動し、管理・監査対象計算機32上にセキュリティ管理部139を構築する(ステップS2308)。

セキュリティ管理部139は、自身を管理・監査対象計算機32上に構築した管理プログラムに対応付けられている情報セキュリティポリシーが示すセキュリティ施策に従った処理を実行する。たとえば、図12に示したような、セキュリティ状態の設定変更などの管理画面を、ネットワーク33を介して、セキュリティポリシー管理・監査装置31'に表示装置16に表示させ、管理者にセキュリティ状態の設定変更内容を入力を促す。そして、管理者より受け付けたセキュリティ状態の設定変更内容を、ネットワーク33を介して、セキュリティポリシー管理・監査装置31'から入手し、その内容に従ってセキュリティ状態を変更する。

以上により、ユーザが構築した情報システムに、設計フェーズで決定した情報セキュリティポリシー各々のセキュリティ施策が実施されていることを確実にすることができる。

次に、運用フェーズでの動作について説明する。

図26に、運用フェーズでのセキュリティポリシー管理・監査装置31'の動作手順を示す。この手順は、運用フェーズでの処理により、設計フェーズで決定した情報セキュリティポリシー各々のセキュリティ施策が実施されていることが確認された情報システムに対して行われる。

まず、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、図23に示したステップS2301～S2302を定期的に行い(ステップS2601～ステップS2602)、管理・監査対象システムの構成機器情報/セキュリティ状態データベース135の内容を最新状態に更新する。また、入出力制御部114を介して、管理者より監査結果報告指示を受け付けると(ステップS2603)、図23に示したS2304～S2308を実行する(ステップS2604)。

このようにすることで、管理者は、最新状態に更新された管理・監査対象システムの構成機器情報/セキュリティ状態データベース135の内容に基づいて作成された監査結果報告書から、導入フェーズ後に、ソフトウェアのバージョンアップ

やパッチの適用、あるいは、装置型式の変更が行われたシステムや、セキュリティ状態に変更があったシステムを特定することができる。そして、必要に応じて当該システムのセキュリティ状態を変更することが可能となる。

また、管理者は、CERT等のセキュリティ情報機関が公表したセキュリティホール情報と前記監査結果報告書とを照合して、セキュリティホールが見つかったシステムを構築するソフトウェア等、セキュリティ状態を変更する必要があるシステムを特定することができる。そして、必要に応じて当該システムのセキュリティ状態を変更することが可能となる。

さらに、管理者は、前記監査結果報告書から、導入フェーズ後に何ら変更されていないシステムを特定し、当該システムを構築するソフトウェアにバージョンアップ版やパッチが公開されている場合はそれらの適用を促したり、当該システムが稼動する装置に新しい装置型式のものが製品化されている場合は、当該装置をこの新しい装置型式のものに変更するように促すこともできる。

以上、本発明の第2実施形態について説明した。

なお、本実施形態では、設計、導入および運用フェーズのそれぞれにおいて用いるセキュリティポリシー管理・監査装置31'は、同じものであることを前提に説明した。しかしながら、設計フェーズにおいてセキュリティ仕様書を作成し出力する装置（図21のステップS2101～S2106をまでの処理を行う装置）は、セキュリティポリシー管理・監査装置31'とは別に設けた装置であってもよい。

すなわち、図18において、少なくとも、管理・監査対象領域制御部111、情報セキュリティポリシー選択制御部112および入力力制御部114を構築し、かつ、システムの構成機器情報データベース131、情報セキュリティポリシー132およびセキュリティ管理・監査プログラムデータベース135を、外部記憶装置13等に形成することができる情報セキュリティポリシー管理・監査支援プログラム134が搭載された電子計算機を用いて、ユーザより指示された情報システムの仕様に従い、セキュリティ仕様書を作成して、これをユーザに提示する。そして、ユーザが決定した、情報システムに適用する情報セキュリティポリシーをセキュリティポリシー管理・監査装置31'に入力することで、当該情報セキュリティポリシーの実施状況を監査する監査プログラムとその状況を変更する管理プログラムとを、

セキュリティポリシー管理・監査装置31'に設定するようにしてもよい。

さて、本実施形態によれば、上記の第1の実施形態の効果に加え、管理者に、情報セキュリティポリシーならびにセキュリティシステムに関する高度な専門知識がなくても、当該管理者が情報セキュリティポリシーの作成、情報セキュリティポリシーに従った情報システムのセキュリティシステムの導入および運用管理といった一連の手順を実施できるように支援にすることが可能となる。

なお、本発明は上記の各実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

例えば、上記の各実施形態では、管理・監査プログラムを管理・監査対象計算機32上に配置したが、これらをネットワーク33を介して管理・監査対象計算機32上のシステムを管理・監査する、いわゆるマネージャ・エージェント型プログラムとして構成し、これらを情報セキュリティポリシー管理・監査支援装置31、31'上に配置するようにしてもよい。

また、上記の各実施形態において、管理プログラムや監査プログラム自身が、ウイルスチェックやパスワードの変更やログの収拾など、情報セキュリティポリシーに関わるその他の処理を実行するようにしてもよいし、あるいは、これらの処理を行うプログラムの実行を、管理プログラムや監査プログラムが管理・監査するようにしてもよい。

以上のように、本発明によれば、情報セキュリティポリシーに従った、情報システムのセキュリティの状態の制御や管理を簡単にすることができる。また、情報セキュリティポリシーならびにセキュリティシステムに関する高度な専門知識がなくても、情報セキュリティポリシーの作成、情報セキュリティポリシーに従ったセキュリティシステムの情報システムへの導入および運用管理といった一連の手順を実施できるように支援することができる。

CLAIMS

1. 情報システムを構成する複数の被管理対象システムのセキュリティ状態を、セキュリティ施策のポリシーを表す情報セキュリティポリシーに従って制御するセキュリティ管理システムであって、

少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキュリティ状態を、当該対応する情報セキュリティポリシーに整合するように制御する、複数の管理部と、

情報セキュリティポリシー、被管理対象システムおよび管理部の対応を登録したデータベースと、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付部と、

前記データベースから、前記セキュリティ内容受付部が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている管理部を抽出する抽出部と、

前記抽出部が抽出した管理部に、当該管理部に対応する被管理対象システムのセキュリティ状態を、当該管理部に対応する情報セキュリティポリシーに整合するように変更させる管理制御部と、を有する。

2. 情報システムを構成する複数の被管理対象システムの、セキュリティ施策のポリシーを表す情報セキュリティポリシーに関わるセキュリティ状態を監査するセキュリティ管理システムであって、

少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティ状態を監査する、複数の監査部と、

情報セキュリティポリシー、被管理対象システムおよび監査部の対応を登録したデータベースと、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付部と、

前記データベースから、前記セキュリティ内容受付部が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている監査部を抽出する抽出部と、

前記抽出部が抽出した監査部に、当該監査部に対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティ状態を監査させる監査制御部と、を有する。

3. 情報システムを構成する複数の被管理対象システムのセキュリティ状態を、セキュリティ施策のポリシーを表す情報セキュリティポリシーに従って制御するセキュリティ管理システムであって、

少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキュリティ状態を、当該対応する情報セキュリティポリシーに整合するように制御する、複数の管理部と、

少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティ状態を監査する、複数の監査部と、

情報セキュリティポリシー、被管理対象システム、管理部および監査部の対応を登録したデータベースと、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付部と、

前記データベースから、前記セキュリティ内容受付部が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている管理部と監査部を抽出する抽出部と、

前記抽出部が抽出した管理部に、当該管理部に対応する被管理対象システムのセキュリティ状態を、当該管理部に対応する情報セキュリティポリシーに整合するように変更させる管理制御部と、

前記抽出部が抽出した監査部に、当該監査部に対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティの状態を監査させる監査制御部と、を有する。

4. 電子計算機を用いて、情報システムを構成する複数の被管理対象システムのセキュリティ状態を、セキュリティ施策のポリシーを表す情報セキュリティポリシーに従って制御するセキュリティ管理方法であって、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるステップと、

予め記憶された、少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキュリティ状態を当該対応する情報セキュリティポリシーに整合するように制御する処理が記述された、複数の管理プログラムから、選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応する管理プログラムを抽出するステップと、

抽出した管理プログラムを実行させ、当該管理プログラムに対応する被管理対象システムのセキュリティ状態を、当該管理プログラムに対応する情報セキュリティポリシーに整合するように変更させるステップと、を有する。

5. 電子計算機を用いて、情報システムを構成する複数の被管理対象システムの、セキュリティ施策のポリシーを表す情報セキュリティポリシーに関わるセキュリティ状態を監査するセキュリティ管理方法であって、

ユーザより、情報セキュリティポリシーと被管理対象システムの範囲の選択を受け付けるステップと、

予め記憶された、少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティ状態を監査する処理が記述された、複数の監査プログラムから、選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている監査プログラムを抽出するステップと、

抽出した監査プログラムを実行させ、当該監査プログラムに対応する被管理対象システムの当該監査プログラムに対応する情報セキュリティポリシーに関わる

セキュリティ状態を監査させるステップと、を有する。

6. 情報システムを構成する複数の被管理対象システムのセキュリティ状態を、セキュリティ施策のポリシーを表す情報セキュリティポリシーに従って制御するためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読み取られて実行されることで、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付部と、

少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキュリティ状態を当該対応する情報セキュリティポリシーに整合するように制御する処理が記述された複数の管理プログラムを格納するデータベースから、前記セキュリティ内容受付部が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応する管理プログラムを抽出する抽出部と、

前記抽出部が抽出した管理プログラムを実行させ、当該管理プログラムに対応する被管理対象システムのセキュリティ状態を、当該管理プログラムに対応する情報セキュリティポリシーに整合するように変更させる管理制御部とを、前記電子計算機上に構築する。

7. 情報システムを構成する複数の被管理対象システムの、セキュリティ施策のポリシーを表す情報セキュリティポリシーに関わるセキュリティ状態を監査するためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読み取られて実行されることで、

ユーザより、情報セキュリティポリシーと被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付部と、

少なくとも1つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティ状態を監査する処理が記述された複数の監査プログラムを格納するデータベースから、前記セキュリティ内容受付部が選択を受け付けた範

囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている監査プログラムを抽出する抽出部と、

前記抽出部が抽出した監査プログラムを実行させ、当該監査プログラムに対応する被管理対象システムの当該監査プログラムに対応する情報セキュリティポリシーに関わるセキュリティ状態を監査させる監査制御部とを、前記電子計算機上に構築する。

8. 電子計算機を用いて、情報システムを構成する複数の被管理対象システムのセキュリティ管理を支援するセキュリティ管理方法であって、

セキュリティ施策のポリシーを表す情報セキュリティポリシーと、少なくとも1つの被管理対象システムとの対応が記述されたデータベースから、ユーザより指定された情報システムを構成する被管理対象システム各々に対応付けられている情報セキュリティポリシーを抽出して、当該情報システムに適用すべきセキュリティ仕様を策定するセキュリティ仕様策定ステップと、

前記セキュリティ仕様策定ステップで策定されたセキュリティ仕様により特定される情報セキュリティポリシーおよび被管理対象システムの組の各々に対応付けられて記憶された、当該被管理対象システムの型式やソフトウェアバージョンといった諸情報、および、当該被管理対象システムの当該情報セキュリティポリシーに関わるセキュリティ状態を監査するための処理が記述された複数の監査プログラムを実行し、前記ユーザより指定された情報システムを構成する被管理対象システム各々の型式やソフトウェアバージョンといった諸情報およびセキュリティ状態を監査して、前記情報システムのセキュリティを診断するセキュリティ診断ステップと、

前記セキュリティ仕様策定ステップで策定されたセキュリティ仕様により特定される情報セキュリティポリシーおよび被管理対象システムの組の各々に対応付けられて記憶された、当該被管理対象システムの当該情報セキュリティポリシーに関わるセキュリティ状態を制御する処理が記述された複数の管理プログラムの中から、ユーザにより指定された管理プログラムを実行し、当該管理プログラムに対応する被管理対象システムのセキュリティ状態を、当該管理プログラムに対

応する情報セキュリティポリシーに整合するように変更させるセキュリティ運用管理ステップと、を有する。

9. 請求項8記載のセキュリティ管理方法であって、

前記セキュリティ診断ステップは、

情報セキュリティポリシーと、被管理対象システムと、前記被管理対象システムの型式やソフトウェアバージョンといった諸情報および前記被管理対象システムの前記情報セキュリティポリシーに関わるセキュリティ状態を監査する処理が記述された監査プログラムとの対応が記述されたデータベースから、前記セキュリティ仕様策定ステップで策定されたセキュリティ仕様により特定される情報セキュリティポリシーおよび被管理対象システムの組の各々に対応付けられている監査プログラムを抽出して実行することにより、前記ユーザより指定された情報システムのセキュリティを診断し、

前記セキュリティ運用管理ステップは、

情報セキュリティポリシーと、被管理対象システムと、前記被管理対象システムのセキュリティの前記情報セキュリティポリシーに関わるセキュリティ状態を制御する処理が記述された管理プログラムとの対応が記述されたデータベースから、前記セキュリティ仕様策定ステップで策定されたセキュリティ仕様により特定される情報セキュリティポリシーおよび被管理対象システムの組の各々に対応付けられている管理プログラムを抽出し、さらにその中からユーザにより指定された管理プログラムを抽出して実行することにより、当該管理プログラムに対応する被管理対象システムのセキュリティ状態を、当該管理プログラムに対応する情報セキュリティポリシーに整合するように変更させる。

10. 請求項8記載のセキュリティ管理方法であって、

前記セキュリティ診断ステップは、定期的に実行される。

11. 請求項8記載のセキュリティ管理方法であって、

前記管理プログラムは、

ユーザより受け付けた設定内容に従って、当該管理プログラムに対応する被管理対象システムのセキュリティ状態を、当該管理プログラムに対応する情報セキュリティポリシーに整合するように変更する。

1 2. 請求項 8 記載のセキュリティ管理方法であって、

情報セキュリティポリシーと少なくとも 1 つの被管理対象システムとの対応が記述されたデータベース、および、情報セキュリティポリシーと被管理対象システムとの組に各々対応付けられて記憶された監査/管理プログラムには、CERT (Computer Emergency Response Team) 等のセキュリティ情報機関が公表したセキュリティホール情報、および、ユーザより指定された情報システムに対して実施した前記セキュリティ診断ステップでの診断結果が反映される。

1 3. 情報システムを構成する複数の被管理対象システムのセキュリティ管理を支援するセキュリティ管理システムであって、

セキュリティ施策のポリシーを表す情報セキュリティポリシーと、少なくとも 1 つの被管理対象システムとの対応が記述されたデータベースと、

ユーザより指定された情報システムを構成する被管理対象システム各々に対応付けられている情報セキュリティポリシーを前記データベースから抽出して、当該情報システムに適用すべきセキュリティ仕様を策定するセキュリティ仕様策定部と、

前記セキュリティ仕様策定部で策定されたセキュリティ仕様により特定される情報セキュリティポリシーおよび被管理対象システムの組の各々に対応付けられて設けられた、当該被管理対象システムの型式やソフトウェアバージョンといった諸情報、および、当該被管理対象システムの当該情報セキュリティポリシーに関わるセキュリティ状態を監査する複数の監査部と、

前記複数の監査部での監査結果に基づいて、前記ユーザより指定された情報システムのセキュリティを診断するセキュリティ診断部と、

前記セキュリティ仕様策定ステップで策定されたセキュリティ仕様により特定される情報セキュリティポリシーおよび被管理対象システムの組の各々に対応付

けられて設けられた、当該被管理対象システムの当該情報セキュリティポリシーに関わるセキュリティ状態を制御する複数の管理部と、

ユーザより指定された管理部を実行して、当該管理プログラムに対応する被管理対象システムのセキュリティ状態を、当該管理プログラムに対応する情報セキュリティポリシーに整合するように変更させるセキュリティ運用管理部と、を有する。

ABSTRACT

情報セキュリティポリシーに従った企業情報システムのセキュリティ管理・監査を簡単にする。情報セキュリティポリシーおよび対象システムと管理・監査プログラムを対応づけたセキュリティ管理・監査プログラムデータベース133を設ける。操作者により指定された情報セキュリティポリシーおよび対象システムの範囲に対応する管理・監査プログラムを検索し、自動的に実行する。管理・監査プログラムは、自身に対応する対象システムの情報セキュリティポリシーに関する管理・監査を行う。